

## BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement is made and entered into effective as of the \_\_\_ day of \_\_\_\_\_, \_\_\_\_, by and between \_\_\_\_\_, ("Business Associate"), and \_\_\_\_\_, ("Covered Entity"). In consideration of the mutual promises below, and other good and valuable consideration, the sufficiency of which is hereby acknowledged, the parties agree as follows:

### 1. DEFINITIONS

Terms used in this Agreement that are specifically defined in HIPAA shall have the same meaning as set forth in HIPAA. A change to HIPAA which modifies any defined HIPAA term, or which alters the regulatory citation for the definition shall be deemed incorporated into this Agreement.

- (a) **"Business Associate"** shall mean the above-stated "Business Associate." It shall also have the meaning given to such term under the Privacy Rule, including but not limited to 45 CFR Section 160.103.
- (b) **"Covered Entity"** shall mean the above stated "Covered Entity". It shall also have the meaning given to the term under the Privacy Rule, including but not limited to 45 CFR Section 160.103.
- (c) **"Data Aggregation"** shall have the meaning given to the term under the Privacy Rule, including but not limited to 45 CFR Section 164.501.
- (d) **"Designated Record Set"** shall have the meaning given to the term under the Privacy Rule, including but not limited to 45 CFR Section 164.501.
- (e) **"Electronic Protected Health Information"** or **"EPHI"** shall have the same meaning as the term "electronic protected health information" in 45 C.F.R. § 160.103, and is EPHI that is created, received, maintained or transmitted by or on behalf of Covered Entity or its affiliates or by Business Associate.
- (f) **"HIPAA"** means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-91, as amended, and related HIPAA regulations (45 C.F.R. Parts 160-164).
- (g) **"HITECH"** means the Health Information Technology for Economic and Clinical Health Act, found in Title XIII of the American Recovery and Reinvestment Act of 2009, Public Law 111-005.
- (h) **"Individual"** shall have the same meaning as the term "individual" in 45 C.F.R. § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).
- (i) **"Privacy Rule"** shall mean the HIPAA Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. part 160 and part 164, subparts A and E.
- (j) **"Protected Health Information"** or **"PHI"** shall have the same meaning as the term "protected health information" in 45 C.F.R. § 160.103, and is PHI that is created, received, maintained or transmitted by or on behalf of Covered Entity or its affiliates or by Business Associate. All references to PHI shall also include EPHI, unless otherwise stated in this Agreement.
- (k) **"Required By Law"** shall have the same meaning as the term "required by law" in 45 C.F.R. § 164.103.
- (l) **"Secretary"** shall mean the Secretary of the Department of Health and Human Services or his designee.
- (m) **"Security Incident"** shall have the same meaning as the term "security incident" in 45 C.F.R. § 164.304.
- (n) **"Security Rule"** shall mean the HIPAA Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. § 164, subpart C.
- (o) **"Unsecured PHI"** shall have the same definition that the Secretary gives the term in guidance issued pursuant to § 13402 of HITECH.

## 2. OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

Business Associate agrees to:

- (a) Not use or disclose PHI other than as permitted or required by this Agreement, or as required by law.
- (b) Use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by this Agreement.
- (c) Report to Covered Entity any use or disclosure of PHI or EPHI not permitted by this Agreement of which it becomes aware or should have known, and any Security Incident of which it becomes aware. Business Associate will make the report to the Covered Entity's Privacy Official and Security Officer or to an authorized person in the Covered Entity's legal department as soon as reasonably practicable. This report will include at least the following information: (a) the nature of the non-permitted or violating use or disclosure or Security Incident; and (b) the PHI and EPHI used or disclosed.
- (d) Develop, implement, maintain, and use appropriate safeguards to prevent any use or disclosure of the PHI or EPHI other than as provided by this Agreement, and to implement administrative, physical, and technical safeguards as required by sections 164.308, 164.310, 164.312 and 164.316 of title 45, Code of Federal Regulations and HITECH to protect the confidentiality, integrity, and availability of EPHI or PHI that Business Associate creates, receives, maintains, or transmits, in the same manner that such sections apply to the Covered Entity. *See* HITECH § 13401.
- (e) Comply with any additional requirements of Title XIII of HITECH that relate to privacy and security and that are made applicable with respect to covered entities. *See* HITECH § 13401.
- (f) Adopt the technology and methodology standards required in any guidance issued by the Secretary pursuant to HITECH §§ 13401-13402.
- (g) Mitigate any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement and notify Covered Entity of any breach of Unsecured PHI, as required under HITECH § 13402.
- (h) In the case of a breach of Unsecured PHI, following the discovery of a breach of such information, notify Covered Entity of such breach. The notice shall include the identification of each individual whose Unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, or disclosed during the breach.
- (i) Enter into an agreement with each of its subcontractors pursuant to 45 CFR § 164.308(b)(1) and HITECH § 13401 that is appropriate and sufficient to require each such subcontractor to protect PHI to the same extent required by Business Associate hereunder.
- (j) Along with its agents or subcontractors, if any, only request, use and disclose the minimum amount of PHI necessary to accomplish the purpose of the request, use or disclosure. Business Associate agrees to comply with the Secretary's guidance on what constitutes "minimum necessary". *See* HITECH § 13405.
- (k) Take reasonable steps to cure the breach or end the violation if Business Associate knows of a pattern of activity or practice by Covered Entity that constitutes a material breach or violation of Covered Entity's obligations under this Agreement. If such steps are unsuccessful within a period of 30 days, Business Associate will either: 1) terminate the Agreement, if feasible; or 2) report the problem to the Secretary. *See* HITECH § 13404(b).
- (l) Ensure that any agent, including a subcontractor, to whom it provides PHI or EPHI agrees in writing to the same restrictions and conditions that apply to Business Associate in this Agreement related to such information.

(m) Provide, at the request of Covered Entity, within 30 days of receipt of the request, access to PHI in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 C.F.R. 164.524 if Business Associate maintains PHI in a designated record set as defined by the Privacy Rule.

(n) Make any amendment(s) to PHI in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 C.F.R. 164.526 at the request of an Individual, within 30 days of receipt of the direction or agreement from the Covered Entity, if Business Associate maintains PHI in a designated record set as defined by the Privacy Rule.

(o) Make its internal practices, books, and records, including policies and procedures, relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of Covered Entity available to the Covered Entity, or to the Secretary, within 30 days of receipt of a request from the Covered Entity for such disclosure, or person designated by the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule and Security Rule.

(p) Document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. 164.528.

(q) Provide to Covered Entity or an Individual, within 30 days of a request for an accounting of disclosures, information collected in accordance with subsection (2)(p) of this Agreement, to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. 164.528. Except in the case of a direct request from an Individual for an accounting related to treatment, payment, or operations disclosures through an electronic health record, if the request for an accounting is delivered directly to Business Associate or its agents or subcontractors, if any, Business Associate shall within ten (10) business days of a request notify Covered Entity about such request. Covered Entity shall either request that Business Associate provide such information directly to the Individual, or it shall request that the information be immediately forwarded to Covered Entity for compilation and distribution to such Individual. In the case of a direct request for an accounting from an Individual related to treatment, payment, or operations disclosures through electronic health records, Business Associate shall provide such accounting to the Individual in accordance with HITECH § 13405(c). Business Associate shall not disclose any PHI unless such disclosure is Required by Law or is in accordance with this Agreement. Business Associate shall document such disclosures. Notwithstanding anything in the Agreement to the contrary, Business Associate and any agents or subcontractors shall continue to maintain the information required for purposes of complying with this Section 2.7 for a period of six (6) years after termination of the Agreement.

### **3. PERMITTED USES AND DISCLOSURES BY BUSINESS ASSOCIATE**

(a) Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI on behalf of, or to provide services to, Covered Entity as long as such use or disclosure of PHI would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

(b) Except as otherwise limited in this Agreement, Business Associate may disclose PHI for the proper management and administration of Business Associate provided that the disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(c) Except as otherwise limited in this Agreement, Business Associate may use PHI to provide Data Aggregation services to Covered Entity as permitted by 42 C.F.R. 164.504(e)(2)(i)(B).

(d) Business Associate may use PHI to report violations of law to appropriate Federal and State authorities, consistent with Sec. 164.502(j)(1).

**4. OBLIGATIONS OF COVERED ENTITY TO INFORM BUSINESS ASSOCIATE OF PRIVACY PRACTICES AND RESTRICTIONS**

(a) Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 C.F.R. 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

(b) Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose PHI, to the extent that such changes may affect Business Associate's use or disclosure of PHI.

(c) Covered Entity shall notify Business Associate of any restriction on the use or disclosure of PHI that Covered Entity has agreed to or must comply with in accordance with 45 C.F.R. 164.522 and/or HITECH § 13405(a), to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

(d) Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule or Security Rule if done by Covered Entity.

**5. TERMS AND TERMINATION**

(a) **Term.** The Term of this Agreement shall be effective as of the date of the Agreement, and shall terminate when all of the PHI and EPHI provided by Covered Entity to Business Associate or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy PHI and EPHI, protections are extended to such information, in accordance with the termination provisions in this Section.

(b) **Termination for Cause.** Upon Covered Entity's knowledge of a material breach by Business Associate Covered Entity shall either:

(1) Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement if Business Associate does not cure the breach or end the violation within 30 days;

(2) Immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and cure is not possible; or

(3) If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.

(c) **Effect of Termination.**

(1) Except as provided in paragraph (2) of this Section 5(c), upon termination of this Agreement, for any reason, Business Associate shall return or destroy all PHI and EPHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to PHI and EPHI that is in the possession of subcontractors or agents of Business Associate shall retain no copies of the PHI and EPHI.

(2) In the event that Business Associate determines that returning or destroying the PHI or EPHI is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon the determination by Business Associate that return or destruction of PHI or EPHI is infeasible, Business Associate shall extend the protections of this Agreement to such PHI or EPHI and limit further uses and disclosures of such PHI or EPHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI or EPHI.

**6. MISCELLANEOUS**

(a) **Regulatory References.** A reference in this Agreement to a section in the HIPAA Privacy Rule or Security Rule means the section as in effect or as amended.

(b) **Agreement.** The Parties agree to take such action as is necessary to amend this Agreement from time-to-time as is necessary for Covered Entity to comply with the requirements of the HIPAA Privacy Rule, Security Rule, and related provisions.

(c) **Conflict.** This Agreement and any underlying services agreement are the only agreement between the parties related to the subject matter in this Agreement. To the extent there is any inconsistency between the terms and conditions of this Agreement and any services agreement, the terms and conditions of the Agreement shall govern.

(d) **Binding Effect.** This Agreement is binding upon the successors and assigns of the parties herein. This Agreement is intended to confer rights and responsibilities only on the Covered Entity and Business Associate and does not create or vest rights or remedies in any third party.

(e) **Enforceability.** If any provision hereof shall be declared to be invalid or unenforceable, such declaration of invalidity or unenforceability shall not affect any remaining provisions hereof which can be given effect.

(f) **Relationship of the Parties.** Nothing in this Agreement shall create any relationship between Covered Entity and Business Associate other than as independent contractors. No employee or agent of either party may be deemed an employee or agent of the other party by reason of this Agreement.

(g) **Survival.** Business Associate's obligation to protect the confidentiality of the Protected Health Information, including the requirements in section 6(d) shall survive the termination of this Agreement and shall continue for as long as Business Associate maintains Protected Health Information.

(h) **Construction.** This Agreement shall be governed by the law of the state of the Covered Entity's headquarters without respect to its conflict of law principles.

This Agreement is entered into by the parties as of the first date set forth above.

**COVERED ENTITY**

**BUSINESS ASSOCIATE**

By: \_\_\_\_\_

By: \_\_\_\_\_

Name: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Title: \_\_\_\_\_

These materials may be reproduced and used only by long-term health care providers and their health care affiliates for their internal use, in connection with their efforts to comply with relevant legal rules and regulations. All other reproduction, transfer and use is prohibited without the express written consent of the LTCC. These materials are for informational purposes only and do not constitute legal advice or a comprehensive guide to issues to be considered when entering into a business associate agreement. Neither the LTCC nor its members make any representation that use of these materials will ensure legal compliance.